This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

Claim 1 (Currently Amended): A method for authorizing a transaction by a user using a terminal which is capable of communicating with a background system, with steps performed by the terminal comprising:

determining non-confidential identification information which identifies the user,

sending terminal data to the background system, the terminal data serving to authenticate the terminal at the background system, the terminal data comprising ~~and to transmit~~ user identification data from which the identity of the user can be derived, ~~to the background system,~~ wherein the user identification data corresponds to, or has been derived from, the non-confidential identification information determined by the terminal,

receiving secret data assigned to the user from the background system, wherein the secret data pertains to a secret that is known to the user,

presenting the ~~playing back a~~ secret given by the secret data to the user, thus signaling to the user that the terminal can be trusted,

determining a personal feature of the user, and

sending feature data ~~which~~ to the background system, wherein the feature data is related to the personal feature of the user, and wherein the feature data ~~to the background system to signal~~ signals or ~~document~~ documents the authorization of the transaction by the user.

Claim 2 (Currently Amended): The method according to Claim 1, wherein the terminal ~~sends to the background system a message~~ data is secured with at least one of a MAC and a cryptographic signature for authentication at the background system.

Claim 3 (Canceled).

Claim 4 (Currently Amended): The method according to Claim 1, wherein the secret ~~played back~~ that is presented to the user is at least one of a text information, acoustic information, visual information, and tactile information.

Claim 5 (Previously Presented): The method according to Claim 1, wherein transaction data is also displayed to the user.

Claim 6 (Previously Presented): The method according to Claim 1, wherein the personal feature is a biometric feature of the user.

Claim 7 (Previously Presented): The method according to Claim 1, further comprising receiving acknowledgement data from the background system and at least one of displaying and printing out an acknowledgement for the user.

Claim 8 (Currently Amended): A method for authorizing a transaction by a user, the method using a background system capable of communicating with a terminal, with steps performed by the background system comprising:

receiving terminal data from the terminal, the terminal data authenticating the terminal at the background system, the terminal data comprising user identification data from which the identity of the user ~~being derivable from the data~~ can be derived, wherein the user identification data corresponds to, or has been derived from, non-confidential identification identification,

if the authentication of the terminal at the background system has been successful, then accessing secret data stored in a database and assigned to the user, and sending transmission data from which the secret data can be determined to the terminal, wherein the secret data pertains to a secret that is known to the user and that serves to signal to the user that the terminal can be trusted, and

receiving feature data from the terminal, the feature data pertaining at least to a personal feature of the user and documenting the authorization of the transaction by the user.

Claim 9 (Previously Presented): The method according to Claim 8, wherein the secret data pertains to a secret which changes from one transaction to the next.

Claim 10 (Previously Presented): The method according to Claim 9, wherein the secret data pertains to a secret which depends at least in part on transactions performed previously.

Claim 11 (Currently Amended): The method according to Claim 8, wherein the feature data ~~which pertains at least to the personal feature of the user~~ is checked, and the transaction is considered as authorized by the user only if this check is successful.

Claim 12 (Previously Presented): The method according to Claim 11, wherein acknowledgement data is sent to the terminal if the check is successful.

Claim 13 (Currently Amended): A method for authorizing a transaction by a user using a terminal capable of communicating with a background system, with ~~the steps~~ steps comprising:

determining, by the terminal, non-confidential identification information which identifies the user,

communicating between the terminal and the background system to authenticate the terminal at the background system, the communicating comprising that the terminal ~~and to transmit~~ transmits user identification data from which the identity of the user can be derived to the background system, wherein the user identification data corresponds to, or has been derived from, the non-confidential identification information determined by the terminal,

if the authentication of the terminal at the background system has been successful, then the background system accesses secret data stored in a database and assigned to the user, and the background systems sends transmission data from which the secret data can be determined ~~is sent~~ to the terminal, wherein the secret data pertains to a secret that is known to the user,

presenting ~~playing back~~, by the terminal, ~~a secret~~ the secret given by the secret data to the user, thus signaling to the user that the terminal can be trusted,

determining, by the terminal, a personal feature of the user, and

performing the transaction using feature data pertaining at least to the personal feature of the user.

Claim 14 (Previously Presented): The method according to Claim 13, wherein the communication processes between the terminal and the background system are protected from attacks at least in part by at least one of time stamps, sequence numbers, random numbers, and an encryption with a session key.

Claim 15 (Currently Amended): A terminal which is capable of communicating with a background system and which is equipped for authorizing a transaction by a user, wherein the terminal ~~is adapted for~~ comprises:

a first module that is adapted for determining non-confidential identification information which identifies the user,

a second module that is adapted for sending terminal data to the background system, the terminal data serving to authenticate the terminal at the background ~~system and to transmit~~ system, the terminal data comprising user identification data from which the identity of the user can be derived, ~~to the background system,~~ wherein the user identification data corresponds to, or has been derived from, the non-confidential identification information determined by the terminal,

a third module that is adapted for receiving secret data assigned to the user from the background system, wherein the secret data pertains to a secret that is known to the user,

a fourth module that is adapted for presenting the ~~playing back a~~ secret given by the secret data to the user, thus signaling to the user that the terminal can be trusted,

a fifth module that is adapted for determining a personal feature of the user, and

a sixth module that is adapted for sending feature data to the background system, wherein the feature data ~~which~~ is related to the personal feature of the user, and wherein the feature data ~~to the background system to signal~~ signals or ~~document~~ documents the authorization of the transaction by the user.

Claim 16 (Currently Amended): A background system which is capable of communicating with a terminal and which is equipped for authorizing a transaction by a user using the terminal, wherein the background system ~~is adapted for~~ comprises:

a first module that is adapted for receiving terminal data from the terminal, the terminal data authenticating the terminal at the background system, the terminal data comprising user identification data from which the identity of the user ~~being derivable from the data~~ can be derived, wherein the user identification data corresponds to, or has been derived from, non-confidential identification information,

a second module that is adapted for authenticating the terminal at the background system, and that is further adapted for performing, if the authentication of the terminal at the background system has been successful, ~~then~~ an operation of accessing secret data stored in a database and assigned to the user, and an operation of sending transmission data from which

the secret data can be determined to the terminal, wherein the secret data pertains to a secret that is known to the user and that serves to signal to the user that the terminal can be trusted, and

a third module that is adapted for receiving feature data from the terminal, the feature data pertaining at least to a personal feature of the user and documenting the authorization of the transaction by the user.

Claim 17 (Currently Amended): A system comprising a background system and at least one terminal capable of communicating with the background system, ~~the system being equipped for authorizing a transaction by a user,~~ wherein the system ~~is adapted for~~ comprises:

a first module that is a module of the terminal and that is adapted for ~~determining, by the terminal,~~ determining non-confidential identification information which identifies the user,

a second module that is a module of the terminal and that is adapted for sending terminal data to the background system, the terminal data serving ~~communicating between the terminal and the background system~~ to authenticate the terminal at the background ~~system and to transmit~~ system, the terminal data comprising user identification data from which the identity of the user can be derived ~~to the background system~~, wherein the user identification data corresponds to, or has been derived from, the non-confidential identification information determined by the terminal,

a third module that is a module of the background system that is adapted for authenticating the terminal at the background system and for performing, if the authentication of the terminal at the background system has been successful, ~~then~~ an operation in which the background system accesses secret data stored in a database and assigned to the user, and an operation in which the background system sends transmission data from which the secret data can be determined ~~is sent~~ to the terminal, wherein the secret data pertains to a secret that is known to the user,

a fourth module that is a module of the terminal and that is adapted for presenting ~~playing back, by the terminal, a secret~~ the secret given by the secret data to the user, thus signaling to the user that the terminal can be trusted,

a fifth module that is a module of the terminal and that is adapted for ~~determining, by the terminal,~~ determining a personal feature of the user, and

a sixth module that is a module of the terminal and that is adapted for sending feature ~~performing the transaction using~~ data pertaining at least to the personal feature of the user to the background system, wherein the feature data signals or documents that the user has authorized the transaction.

Claim 18 (Currently Amended): A computer program product comprising a physical medium having program instructions for at least one processor of a terminal to cause the at least one processor to execute a method for authorizing a transaction by a user, the terminal being capable of communicating with a background system, with steps performed by the terminal comprising:

determining non-confidential identification information which identifies the user,

sending terminal data to the background system, the terminal data serving to authenticate the terminal at the background system, the terminal data comprising ~~and to transmit~~ user identification data from which the identity of the user can be derived, ~~to the background system~~ wherein the user identification data corresponds to, or has been derived from, the non-confidential identification information determined by the terminal,

receiving secret data assigned to the user from the background system, wherein the secret data pertains to a secret that is known to the user,

presenting the ~~playing back a~~ secret given by the secret data to the user, thus signaling to the user that the terminal can be trusted,

determining a personal feature of the user, and

sending feature data to the background system, wherein the feature data ~~which~~ is related to the personal feature of the user, and wherein the feature data ~~to the background system to signal~~ signals or ~~document~~ documents the authorization of the transaction by the user.

Claim 19 (Currently Amended): A computer program product comprising a physical medium having program instructions for at least one processor of a background system to cause the at least one processor to execute a method for authorizing a transaction by a user, the background system being capable of communicating with a terminal, with steps performed by the background system comprising:

receiving terminal data from the terminal, the terminal data authenticating the terminal at the background system, the terminal data comprising user identification data from with the identity of the user ~~being derivable from the data~~ can be derived, wherein the user identification data corresponds to, or has been derived from non-confidential information,

if the authentication of the terminal at the background system has been successful, then accessing secret data stored in a database and assigned to the user, and sending transmission data from which the secret data can be determined to the terminal, wherein the secret data pertains to a secret that is known to the user and that serves to signal to the user that the terminal can be trusted, and

receiving feature data from the terminal, the feature data pertaining at least to a personal feature of the user and documenting the authorization of the transaction by the user.

Claim 20 (New): The method according to Claim 1, wherein the secret that is presented to the user is at least one of a displayed image, an acoustic output, and tactile information.

Claim 21 (New): The method according to Claim 1, wherein the secret that is presented to the user is easily identified by the user.

Claim 22 (New): The method according to Claim 8, wherein the secret that serves to signal to the user that the terminal can be trusted is at least one of a displayed image, an acoustic output, and tactile information.

Claim 23 (New): The method according to Claim 8, wherein the secret that serves to signal to the user that the terminal can be trusted is easily identified by the user.